

Amendments to the Drawings:

The attached sheet of drawings includes changes to Figures 1, 2A, 2B and 3. These sheets, which include Figures 1, 2A, 2B and 3, replace the original sheets including Figures 1, 2A, 2B and 3.

The Examiner objected to Figures 1, 2A, 2B and 3 because the figures should be designated by a legend such as --PRIOR ART--. To overcome the above objection, Applicant has added the legend -- (CONVENTIONAL ART) -- to Figures 1, 2A, 2B and 3.

The Examiner also objected to Figure 3 and 5 because of the following informalities:

(a) Reference character "516" is used in specification

(page 12, line 26) but "360" is used in FIG. 5 to designated "Fl_{2,3}". To overcome the Examiner's objection to FIG. 5, Applicant has changed reference numeral "360" to --516--.

(b) Reference character "515" is used to designate "FL_{2,2}"

in specification (page 12, line 21) but "Fl_{2,2}" in FIG. 5. To overcome the Examiner's objection to FIG. 5, Applicant has amended the specification on page 12, line 21 to change "FL_{2,2}" to --Fl_{2,2}--.

(c) Reference character "360" is used in FIG. 3 to

designate "ZE2 unit" but "Fl_{2,3}" in FIG. 5. The amendments to FIG. 5 above in (a) will overcome the Examiners objection to FIGs. 3 and 5.

(d) Reference character "360" is used to receive the signal

"RR₁" in the specification (page 6, line 5) but "360" is used to receive the signal "RR₂" in FIG. 3. To overcome the Examiner's objection to FIG. 3, Applicant has amended the specification on page 6, lines 5 and 6 to change "RR₁" to --RR₂--.

Applicant also adds reference --R_{3D}-- to the output of delay (D₇) 620 and --R_{5D}-- to the output of sub-cipher 514, although the Examiner did not make an objection.

Appl. No. 10/679,391
Amdt. dated March 28, 2007
Reply to Office Action of November 28, 2006

Attachment: Replacement Sheets
Annotated Sheets Showing Changes

REMARKS

I. Status of Claims

After the above amendments, claims 1-12 are pending. Claims 1 and 8 are independent.

II. Priority Document

Although the priority document was filed at the U.S. Patent and Trademark Office on the filing date of October 7, 2003, the Examiner did not acknowledge the claim for foreign priority and the receipt of the priority document. Therefore, Applicant requests that the Examiner make such acknowledgement.

III. Claim Objections

The Examiner objected to claim 1 because of informalities by indicating that the claim recited the limitations “the second ciphertext bit stream” in line 9 and “the first ciphertext bit stream in line 10. According to the Examiner, there is insufficient antecedent basis for the above limitations in the claim.

Applicant has amended claim 1 as follows:

performing a first-round of encryption by encrypting the received first and second sub-bit streams with predetermined first encryption codes an odd number of times, and outputting a second ciphertext bit stream having been once more encrypted with a predetermined time delay after first ciphertext bit streams of length n are outputted;

IV. Claim Rejections

Rejection under 35 U.S.C. § 112, second paragraph

The Examiner rejected claim 3 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner indicated that claim 3 recites the limitation “first predetermined encryption codes” in line 1. According to the Examiner, it is unclear whether the limited is intended to be the same as or different from the “first predetermined encryption codes” recited in claim 2.

To overcome the examiner's rejection and to clarify the invention, Applicant has amended claim 3 as follows:

3. (Currently Amended) The encryption apparatus of claim 1, wherein the ~~first~~ predetermined second encryption codes comprises at least one of $KO_{2,1}$, $KO_{2,2}$, $KO_{2,3}$, $KI_{2,1}$, $KI_{2,2}$, and $KI_{2,3}$.

Rejections under 35 U.S.C. § 103(a)

The Examiner rejects claims 1-5 and 7-10 under 35 U.S.C. § 103(a) as being unpatentable over Applicant's admitted prior art (AAPA) in view of 3rd Generation Partnership Project, "Document 2: KASUMI Specification" Release 4, 2001-08-28 (DKS).

With respect to independent claim 1, Applicant disagrees with the Examiner's allegations. Based on Applicant's review of the references, there is nothing in the alleged combination of AAPA and DKS that discloses or teaches a method for "performing a second-round of encryption by encrypting the received the first operated ciphertext bit stream and the second operated ciphertext bit stream having the predetermined time delay with predetermined second encryption codes an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams of length n after once more encrypting the first operated ciphertext bit stream with predetermined second encryption codes," as recited in claim 1.

AAPA discloses an example of FOi units, where FOi denotes an ith FO unit. A second operated ciphertext bit stream (L_4) comprising a predetermined time delay is output to provide a 16 bit signal. However, a first operated ciphertext bit stream (R_3) of AAPA is not output to provide a 16 bit signal. AAPA, on the other hand, outputs a first sub-bit stream ($R_{3D} = R_4$) with a predetermined time delay (D_5) 50 as a 16 bit signal.

In embodiments of the present invention, a second-round encryption is performed by outputting the third and fourth ciphertext bit streams (R_5 and L_7) after receiving the first operated ciphertext bit ($R_3=R_4$) and a second operated ciphertext bit stream ($L_5=L_6$) comprising the predetermined time delay. The **first sub-bit stream ($R_{3D} = R_4$)** with a predetermined time delay (D_5) 50 providing a 16 bit signal of AAPA is not analogous to **the first operated ciphertext bit stream (R_4)** provided for second-round encryption because the first operated

ciphertext bit (R_4) is not delayed with a predetermined time delay. Therefore, AAPA does not disclose or teach performing a second-round encryption by outputting the third and fourth ciphertext bit streams after receiving the **first operated ciphertext bit stream**. Likewise, DKS does not supply the above noted deficiencies of AAPA.

DKS discloses a FO Function in Figure 2. In the first round of encryption, a first and second sub-bit stream is received. A first ciphertext bit stream is generated by encrypting the first sub-bit stream with an encryption code $KO_{i,1}$. However, there is nothing in the first round of encryption of DKS that discloses generating a second ciphertext bit stream by encrypting the second sub-bit stream. Moreover, there is nothing in DKS that discloses a second ciphertext bit stream being output with a predetermined time delay. Accordingly, in the second round of encryption, a second operated bit stream comprising a predetermined time delay is not received because there is nothing in DKS that discloses or teaches a bit stream being output with a predetermined time delay.

In view of the above arguments, the alleged combination of AAPA and DKS does not disclose or teach the claimed elements of independent claim 1. Therefore the rejection of claim 1 should be withdrawn. The rejection of claim 8, which claims “a second ciphering unit for receiving the first operated ciphertext bit stream and the second operated ciphertext bit stream having the predetermined time delay, generating third and fourth ciphertext bit streams of length n by encrypting the first operated ciphertext bit stream and the second operated ciphertext bit stream with predetermined second encryption codes $KO_{2,1}$, $KO_{2,2}$, $KO_{2,3}$, $KI_{2,1}$, $KI_{2,2}$, and $KI_{2,3}$ an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams after once more encrypting the first operated ciphertext bit stream with predetermined second encryption codes,” should be withdrawn for at least the same reasons give above with regard to independent claim 1. Moreover, claims 2-4, 7, 9, 11 and 12, which incorporate the limitations of base claims 1 and 8, should also be withdrawn at least based on the above arguments.

With respect to dependent claim 5, Applicant disagrees with the Examiner’s allegations. Based on our review of the references, there is nothing in the alleged combination of AAPA and DKS that discloses or teaches “generating a second signal by performing a logical exclusive-OR-operation on the first operated ciphertext bit stream and the second encryption code $KO_{2,1}$ to

provide a fourth exclusive-OR operated bitstream, encrypting the fourth exclusive-OR-operated bit stream with the second encryption code $KI_{2,1}$ to provide a third encrypted signal, performing a logical exclusive-OR-operation on the third encrypted signal and the second operated ciphertext bit stream to provide a fifth exclusive-OR operated bitstream; generating the third ciphertext bit stream by performing a logical exclusive-OR-operation on the second operated ciphertext bit stream and the second encryption code $KO_{2,2}$, encrypting the fifth exclusive-OR-operated bit stream with the second encryption code $KI_{2,2}$ to provide a fourth encrypted signal, and performing a logical exclusive-OR-operation on the fifth encrypted signal and the second signal delayed by time required for the encryption;” and “generating the fourth ciphertext bit stream by performing a logical exclusive-OR-operation on the second signal and the second encryption code $KO_{2,3}$, encrypting the sixth exclusive-OR-operated bit stream with the second encryption code $KI_{2,3}$, and performing a logical exclusive-OR-operation on the encrypted signal with the third ciphertext bit stream,” as recited in proposed amended claim 5.

AAPA discloses a first ciphertext bit stream that is delayed by a fifth delay (D_5) and output as a delayed signal (R_{3D}). The delayed signal ($R_{3D} = R_4$) is a first operated ciphertext bit stream. However, there is nothing in AAPA that discloses performing a logical exclusive-OR-operation on the first operated ciphertext bit stream (R_3) and a second encryption code to provide a fourth exclusive-OR-operated bitstream.

In embodiments of the present invention, the first operated ciphertext bit stream ($R_3 = R_4$) is generated by performing a logical exclusive-OR operation on a second encrypted signal (R_{2D}) and a first signal (L_3) generated by performing a logical exclusive-OR operation on a first encrypted signal (L_{2D}) and a second sub-bit stream delayed by time required for the encryption (R_{1D}). A logical exclusive-OR-operation is then performed on the first operated ciphertext bit stream (R_4) and the second encryption code $KO_{2,1}$ to provide a fourth exclusive-OR operated bitstream (R_5). However, the first operated ciphertext bit stream as claimed in the present invention is not a delay signal. According, the **delayed signal ($R_{3D} = R_4$)** of AAPA is not analogous to the **first operated ciphertext bit stream (R_4)** that performs a logical exclusive-OR-operation with the second encryption code $KO_{2,1}$ to provide a fourth exclusive-OR operated bitstream. Likewise, DKS does not supply the above noted deficiencies of AAPA.

DKS discloses a logical exclusive-OR operation is performed on a second sub-bit stream and a second encryption code $KO_{i,2}$ to provide a fourth exclusive-OR operated bitstream (input to $Fli2$). The fourth exclusive-OR-operated bit stream (input to $Fli2$) is encrypted with a second encryption code $KI_{i,2}$ to provide a third encrypted signal. However, a logical exclusive-OR-operation on the third encrypt signal is performed with an encrypted signal (output of $Fli1$) that performs a logical exclusive-OR-operation on a second sub-bit stream. The encrypted signal (output of $Fli1$) that performs a logical exclusive-OR-operation on the **second sub-bit stream** of DKS is not analogous to **the second operated ciphertext bit stream** ($L_5 = L_6$).

In embodiments of the present invention, the second operated ciphertext bit stream ($L_5 = L_6$) is generated by performing a logical exclusive-OR-operation on the third encrypted signal (L_{4D}) and a first sub-bit stream delayed by time required for the encryption (R_{3D}). The second sub-bit stream of DKS is not delayed by time required for encryption. Accordingly, the second sub-bit stream of DKS is not analogous to the first sub-bit stream delayed by time required for the encryption (R_{3D}). Therefore, DKS does not disclose performing a logical exclusive-OR-operation on the third encrypted signal and **the second operated ciphertext bit stream** to provide a fifth exclusive-OR operated bitstream.

Furthermore, the alleged combination of AAPA and DKS does not disclose “generating the third ciphertext bit stream by performing a logical exclusive-OR-operation on the second operated ciphertext bit steam and the second encryption code $KO_{2,2}$, encrypting the fifth exclusive-OR-operated bit stream with the second encryption code $KI_{2,2}$ to provide a fourth encrypted signal, and performing a logical exclusive-OR-operation on the fifth encrypted signal and the second signal delayed by time required for the encryption;” and “generating the fourth ciphertext bit stream by performing a logical exclusive-OR-operation on the second signal and the second encryption code $KO_{2,3}$, encrypting the sixth exclusive-OR-operated bit stream with the second encryption code $KI_{2,3}$, and performing a logical exclusive-OR-operation on the encrypted signal with the third ciphertext bit stream.”

In view of the above arguments, the alleged combination of AAPA and DKS does not disclose or teach the claimed elements of claim 5. Therefore the rejection of claim 5 should be withdrawn. The rejection of claim 10, which claims a second ciphering unit comprising “a

fourth block having a seventh exclusive-OR operator for exclusive-OR-operating the first operated ciphertext bit stream with the second encryption code $KO_{2,1}$, a fourth sub-cipher for encrypting the exclusive-OR-operated bit stream with the second encryption code $KI_{2,1}$, and an eighth exclusive-OR operator for generating a second signal by performing a logical exclusive-OR-operation on the encrypted signal and the second operated ciphertext bit stream; a fifth block having a ninth exclusive-OR operator for exclusive-OR-operating the second operated ciphertext bit stream with the second encryption code $KO_{2,2}$, a fifth sub-cipher for encrypting the exclusive-OR-operated bit stream with the second encryption code $KI_{2,2}$, and a tenth exclusive-OR operator for generating the third ciphertext bit stream by performing a logical exclusive-OR-operation on the encrypted signal and the second signal delayed by time required for the encryption,” and “a sixth block having an eleventh exclusive-OR operator for performing a logical exclusive-OR operation on the second signal with the second encryption code $KO_{2,3}$, a sixth sub-cipher for encrypting the exclusive-OR-operated bit stream with the second encryption code $KI_{2,3}$, and a twelfth exclusive-OR operator for generating the fourth ciphertext bit stream by performing a logical exclusive-OR operation on the encrypted signal and the third ciphertext bit stream,” should be withdrawn for at least the same reasons given above with regard to claim 5.

The Examiner rejects claims 6, 11 and 12 under 35 U.S.C. § 103(a) as being unpatentable over AAPA in view of DKS, in further view of Campbell, Jr.

With respect to dependent claim 6, there is nothing in Campbell, Jr. that discloses or teaches an encryption method in which “each of the encryptions includes first and second sub-encryptions,” as recited.

The Examiner admits that neither AAPA nor DKS discloses the outputs from the first and second sub-encryptions are stored and simultaneously retrieved according to an external clock signal. However, the Examiner alleges that Campbell Jr. discloses the outputs from the first and second sub-encryptions are stored and simultaneously retrieved according to an external clock signal, by referenced FIG. 1A, items 18, 20, 22, FIG. 2; col. 5, lines 66-68 and col. 6, lines 1-7 and 11-16.

Applicant disagrees with the Examiner’s allegation. Campbell, Jr. discloses a device for generating an authenticator code by encrypting contents of a plain text message in accordance

with a unique user supplied authenticator key variable. Campbell, Jr. also discloses a T1 memory (20), loaded with a 16-bit authenticator key variable contained in a K memory (48), that serves as an address input to T2 memory (24), and a T3 memory (18) in which data read out of the T3 memory (18) is combined with six low order bits from a shift register in an exclusive OR gate (26) used to replace previous six low order bit positions of a shift register (14) from a control sequencer (22). The control sequencer 22 controls a read cycle initiated at each memory (see col. 5, line 55 – col. 6, line 34). However that is nothing in Campbell, Jr. that discloses an encryption method in which each of the encryptions includes first and second sub-encryptions. Moreover, there is nothing in Campbell Jr. that discloses that the authenticator key variable provided in T1 memory (20) comprises first and second sub-encryptions.

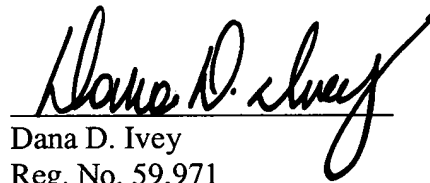
In view of the above arguments, the alleged combination of AAPA, DKS, and Campbell, Jr. does not disclose or teach the claimed elements of claim 6. Therefore, the rejection of claim 6 should be withdrawn.

V. Conclusion

In view of the above, it is believed that the above-identified application is in condition for allowance, and notice to that effect is respectfully requested. Should the Examiner have any questions, the Examiner is encouraged to contact the undersigned at the telephone number indicated below.

Respectfully submitted,

Date: March 28, 2007

A handwritten signature in black ink, appearing to read "Dana D. Ivey", is written over a horizontal line.

Dana D. Ivey
Reg. No. 59,971
Attorney for Applicant

Roylance, Abrams, Berdo & Goodman, L.L.P.
1300 19th Street, N.W., Suite 600
Washington, D.C. 20036-2680
Main: (202) 659-9076
Direct: (202) 530-7372

ANNOTATED SHEET

1/7

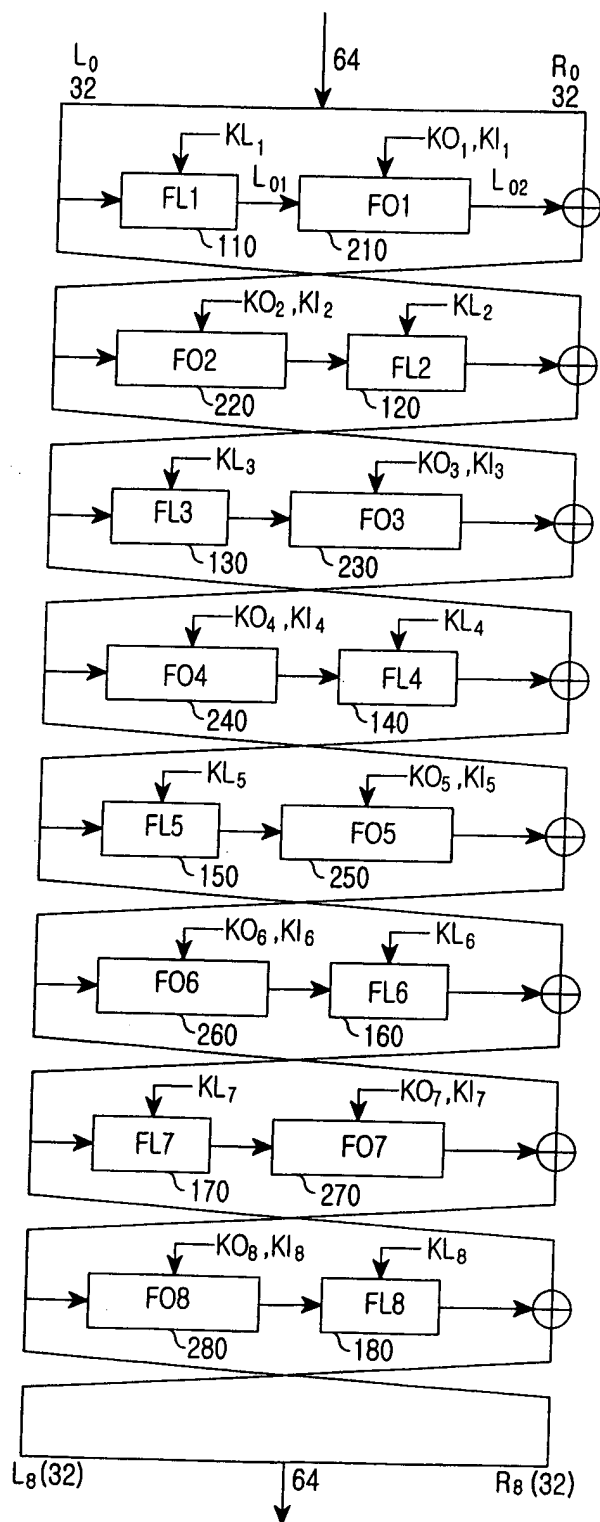


FIG.1
(CONVENTIONAL ART)

ANNOTATED SHEET

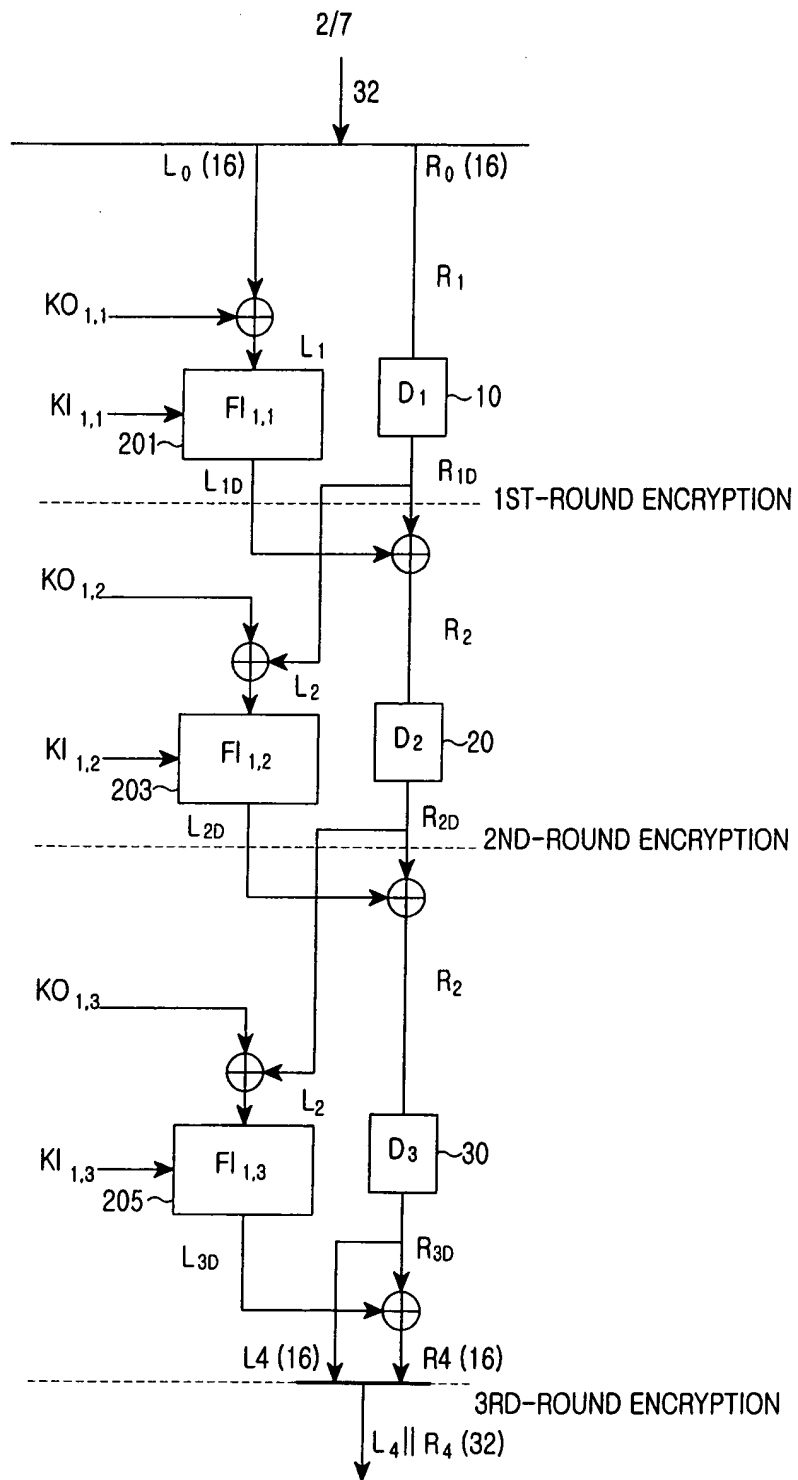


FIG.2A
(CONVENTIONAL ART)

ANNOTATED SHEET

3/7

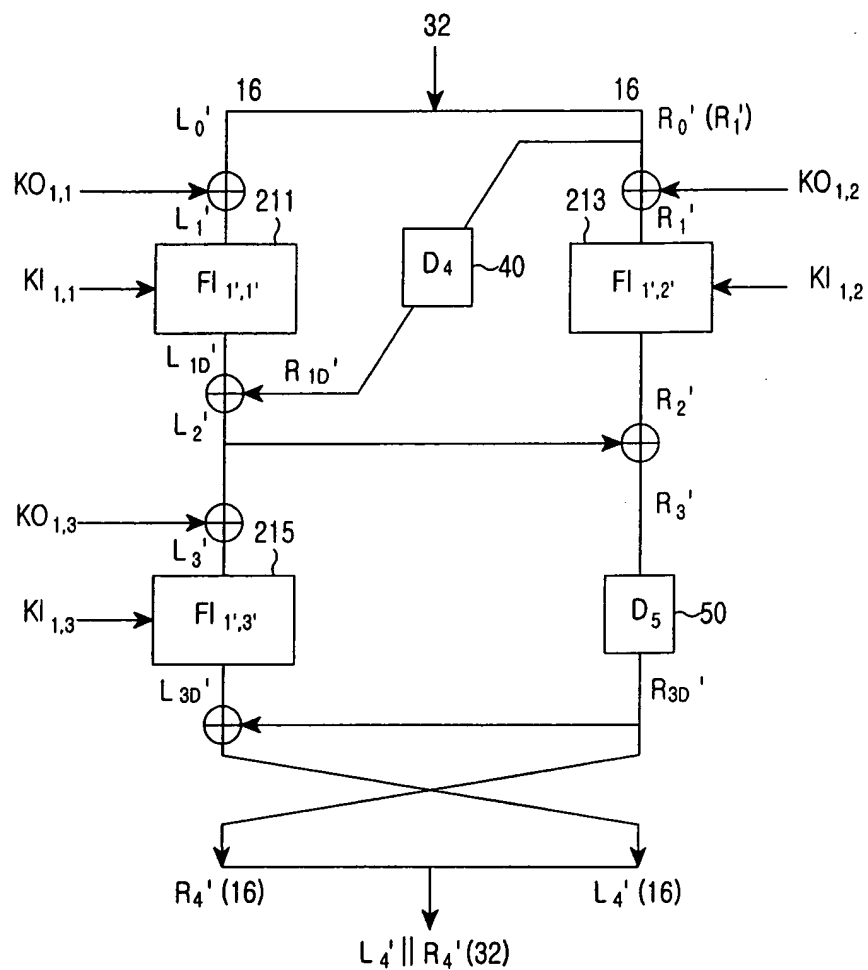


FIG.2B
(CONVENTIONAL ART)

ANNOTATED SHEET

4/7

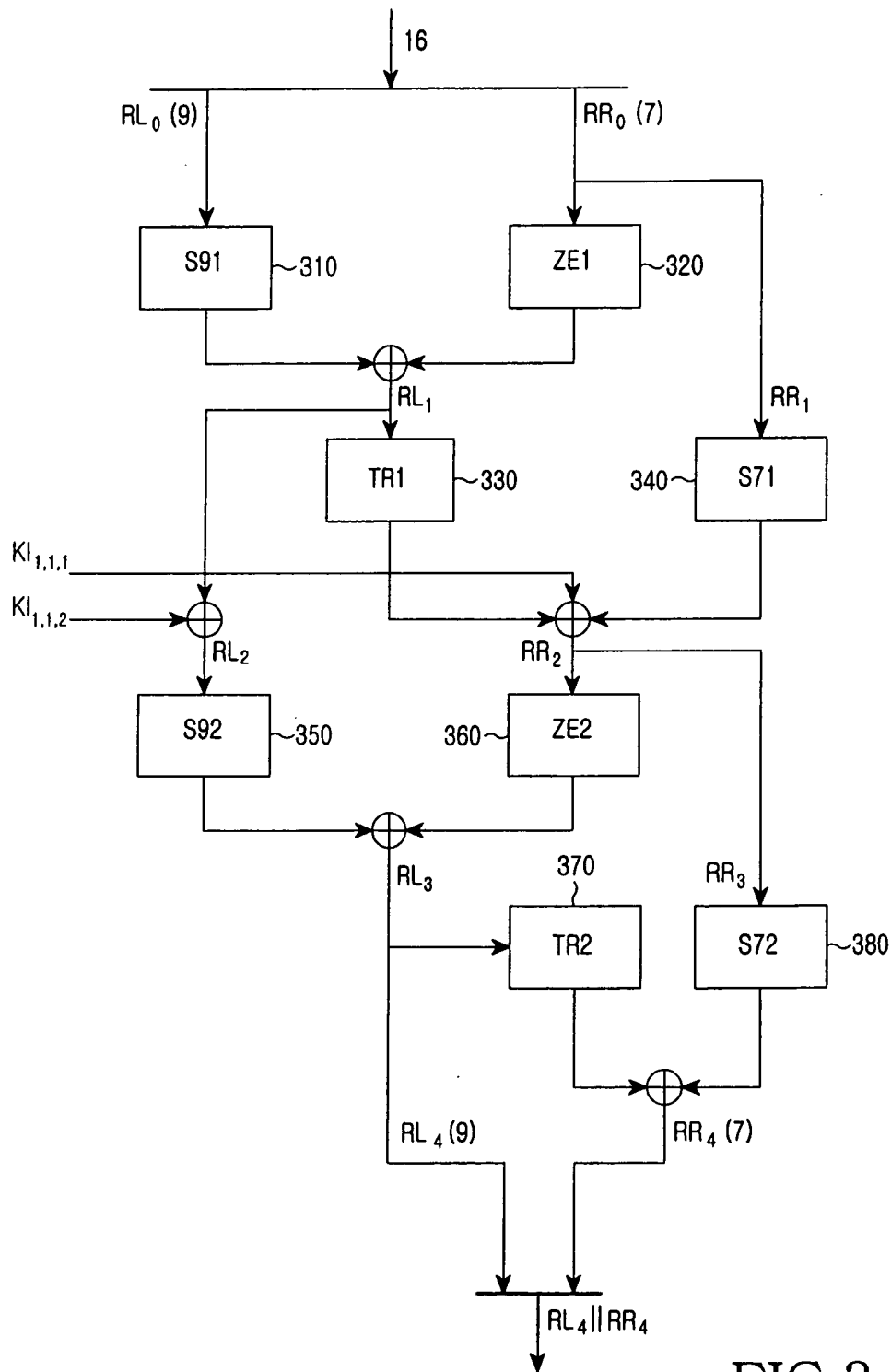


FIG.3
(CONVENTIONAL ART)

ANNOTATED SHEET

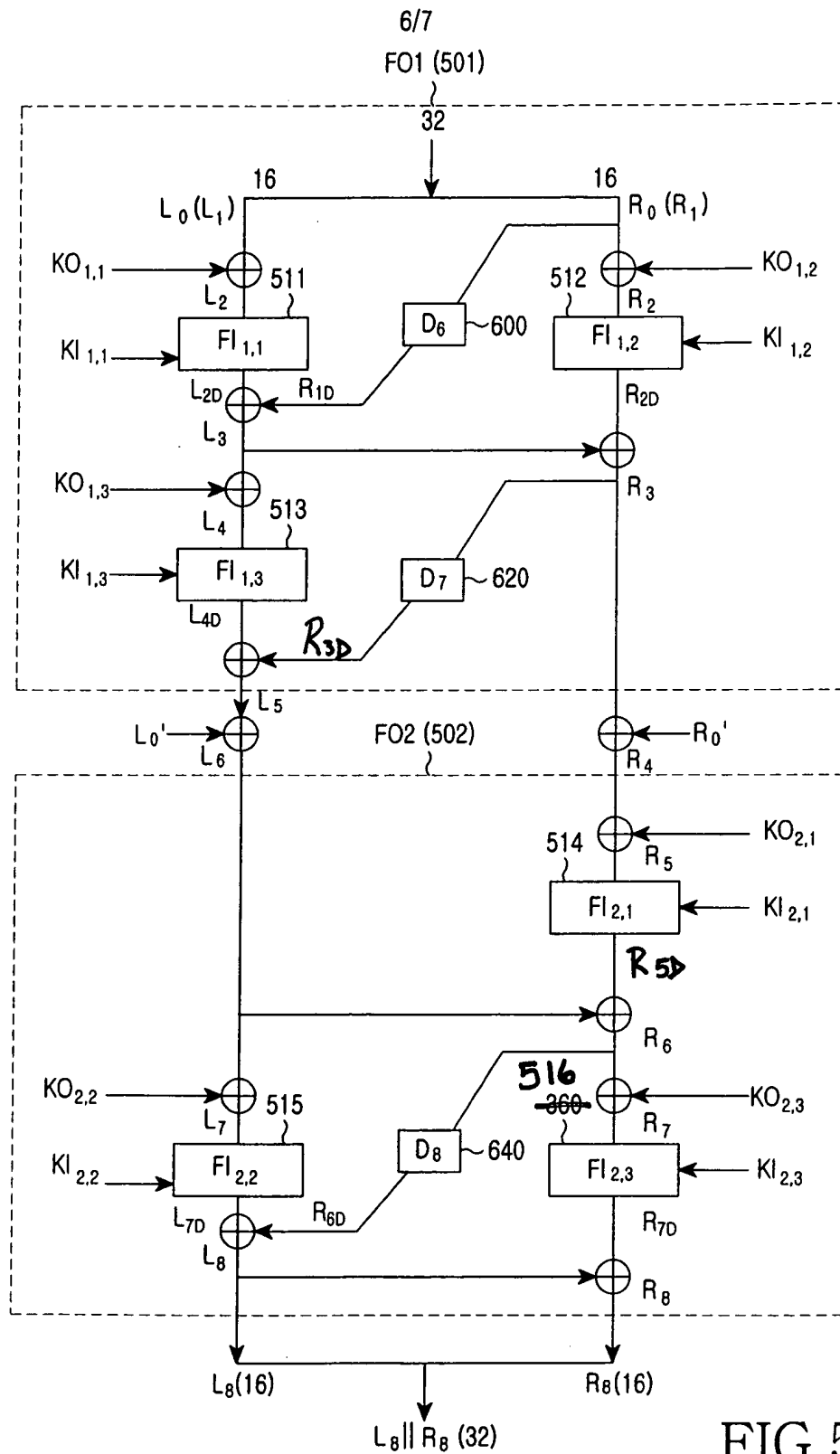


FIG.5